SPYWOLF

Security Audit Report

Completed on

May 18, 2023

OVERVIEW

This audit has been prepared for **PANDA YAYA** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

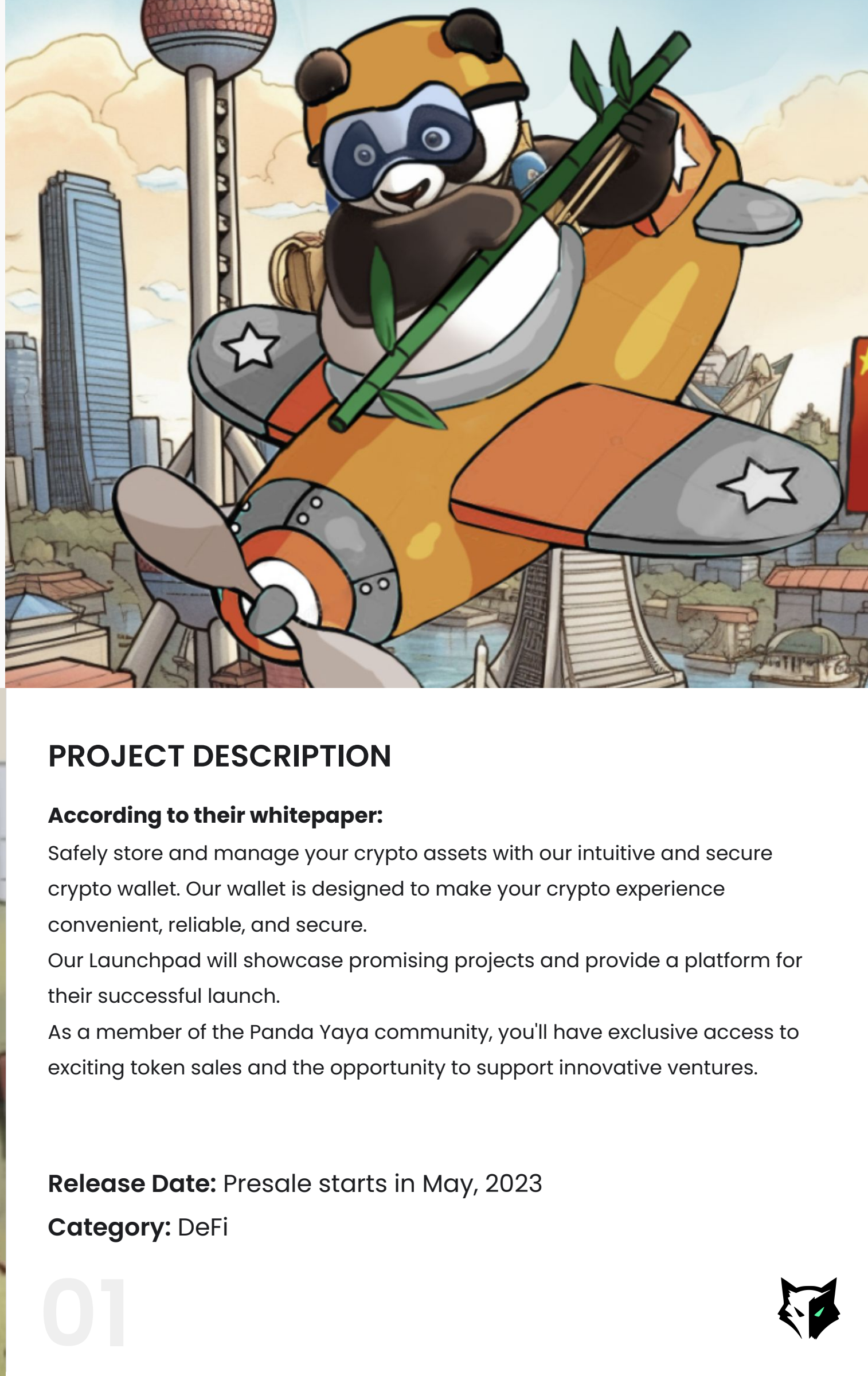
- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

PANDA YAYA



PROJECT DESCRIPTION

According to their whitepaper:

Safely store and manage your crypto assets with our intuitive and secure crypto wallet. Our wallet is designed to make your crypto experience convenient, reliable, and secure.

Our Launchpad will showcase promising projects and provide a platform for their successful launch.

As a member of the Panda Yaya community, you'll have exclusive access to exciting token sales and the opportunity to support innovative ventures.

Release Date: Presale starts in May, 2023

Category: DeFi

CONTRACT INFO

Token Name	Symbol
Panda YAYA	PYY

Contract Address
0x9582B485a673B5470a3FB41B5F8B3504E816aDbf

Network	Language
Binance Smart Chain	Solidity

Deployment Date	Verified?
May 18, 2023	Yes

Total Supply	Status
420,000,000,000,000	Not launched

TAXES

Buy Tax
9%

Sell Tax
9%

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

TOKEN TRANSFERS STATS

Transfer Count	3
Uniq Senders	3
Uniq Receivers	3
Total Amount	10500000000000000.1 PYY
Median Transfer Amount	4200000000000000 PYY
Average Transfer Amount	3500000000000000 PYY
First transfer date	2023-05-18
Last transfer date	2023-05-18
Days token transferred	1

SMART CONTRACT STATS

Calls Count	7
External calls	7
Internal calls	0
Transactions count	7
Uniq Callers	2
Days contract called	1
Last transaction time	2023-05-18 07:34:26 UTC
Created	2023-05-18 07:25:41 UTC
Create TX	0x65cb95563b49c490341899a099cd45e8ccd57831625d340b341dec2e0f6d7a96
Creator	0xffc59f3279d76edb1b90931196746eca0fdd4d60

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ High Risk

Owner can enable/disable trading.
Owner can whitelist address.
Whitelisted addresses are excluded from trading restrictions.

```
function enableTrading(bool _trading) external onlyOwner {
    tradingActive = _trading;
}

function isNotLockBuySell(address _user) public view returns (bool){
    return whitelistBuySell[_user] || tradingActive;
}

function setWhitelistBuySell(address _user, bool _wl) public onlyOwner {
    whitelistBuySell[_user] = _wl;
}

function _transfer(address from, address to, uint256 amount) internal override {
.....................
require(isNotLockBuySell(from), "Panda YAYA: Lock");
.....................
}
```

FOUND THREATS

⚠ High Risk

If reward+rewardCharity+rewardDev are higher than fee , contract will halt and selling will fail.
When rewardAmount+rewardAmountDev+rewardAmountCharity exceeds the feeAmount, contract will halt and selling will fail.

```
function setReward(uint256 total_,uint256 rewardMtk_,
uint256 rewardDev_,uint256 rewardCharity_) external onlyOwner {
    require(total_ <= 20, "Reward fee must less than 20%");
    fee = total_;
    reward = rewardMtk_;
    rewardCharity = rewardCharity_;
    rewardDev = rewardDev_;
}

function _transfer(address from, address to, uint256 amount ) internal override {
.....
uint256 feeInContract = balanceOf(address(this));
if (from != swapPair && !swapping &&
    !isExcludedFromFee[from] && !isExcludedFromFee[to]) {
    swapping = true;
    if(fee > 0 && feeInContract > 0) {
        _swapAndTransferFee(feeInContract);
    }
    swapping = false;
}
.....
}

function _swapAndTransferFee(uint256 feeAmount) private {
uint256 rewardAmount = feeAmount.mul(reward).div(fee);
uint256 rewardAmountDev = feeAmount.mul(rewardDev).div(fee);
uint256 rewardAmountCharity = feeAmount.mul(rewardCharity).div(fee);

uint256 rewardHolder = feeAmount
    .sub(rewardAmount)
    .sub(rewardAmountDev)
    .sub(rewardAmountCharity);
_swapForETH(feeAmount.sub(rewardHolder));
.....
}
```

- Recommendation:
  - Reward, rewardCharity and rewardDev state variables **combined** should be not greater than the fee state variable.
  - rewardAmount+rewardAmountDev+rewardAmountCharity should be not greater than feeAmount
  - _swapForETH() should always accept tokens above 0 as input, because of the router logic

FOUND THREATS

⚠ High Risk

When reward and rewardDev state variables can be out of bonds. The calculated amounts should never be higher than the contract's current BNB balances. If they do, transaction will revert **causing the contract to halt on sell** for regular users (ones not excluded from fees).

```
function _transfer(address from, address to, uint256 amount ) internal override {
.....................................
uint256 feeInContract = balanceOf(address(this));
if (from != swapPair && !swapping &&
    !isExcludedFromFee[from] && !isExcludedFromFee[to]) {
    swapping = true;
    if(fee > 0 && feeInContract > 0) {
        _swapAndTransferFee(feeInContract);
    }
    swapping = false;
}
.....................................
}

function _swapAndTransferFee(uint256 feeAmount) private {
.....................................
    uint256 amount = address(this).balance;
    uint256 marketingAmount = amount.mul(reward).div(5);
    payable(marketing).sendValue(marketingAmount);
    uint256 devAmount = amount.mul(rewardDev).div(5);
    payable(dev).sendValue(devAmount);
    uint256 charityAmount = amount.sub(devAmount).sub(marketingAmount);
    payable(charity).sendValue(charityAmount);
.....................................
}


function sendValue(address payable recipient, uint256 amount) internal {
require(address(this).balance >= amount,"Address: insufficient balance");
(bool success, ) = recipient.call{value: amount}("");
require(success,"Address: unable to send value, recipient may have reverted");
}
```

- Recommendation:
  - Consider another formula for fee tokens distribution.

FOUND THREATS

⚠ Medium Risk

Owner can set buy/sell fees up to 20% and fee distribution ratios without any limitation.
Combined buy+sell = 40%.
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

```
function setReward(uint256 total_,uint256 rewardMtk_,uint256 rewardDev_,
uint256 rewardCharity_) external onlyOwner {
    require(total_ <= 20, "Reward fee must less than 20%");
    fee = total_;
    reward = rewardMtk_;
    rewardCharity = rewardCharity_;
    rewardDev = rewardDev_;
}

function _transfer(address from, address to, uint256 amount ) internal override {
.....................
if (takeFee) {
    uint256 feeAmount = 0;
    if (from == swapPair || to == swapPair) {
        feeAmount = amount.mul(fee).div(100);
    }

    if (feeAmount > 0) {
        super._transfer(from, address(this), feeAmount);
        amount = amount.sub(feeAmount);
    }
}

super._transfer(from, to, amount);
.....................
}
```

- Recommendation:
  - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.

Informational

Owner can exclude address from dividends.
Owner can exclude address from fees.

```
function excludeFromDividends(address account) external onlyOwner {
    dividendTracker.excludeFromDividends(account);
}

function excludeFromFee(address account, bool isExcluded) public onlyOwner {
    isExcludedFromFee[account] = isExcluded;
}
```

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Panda Yaya

GOOD PRACTICES FOUND

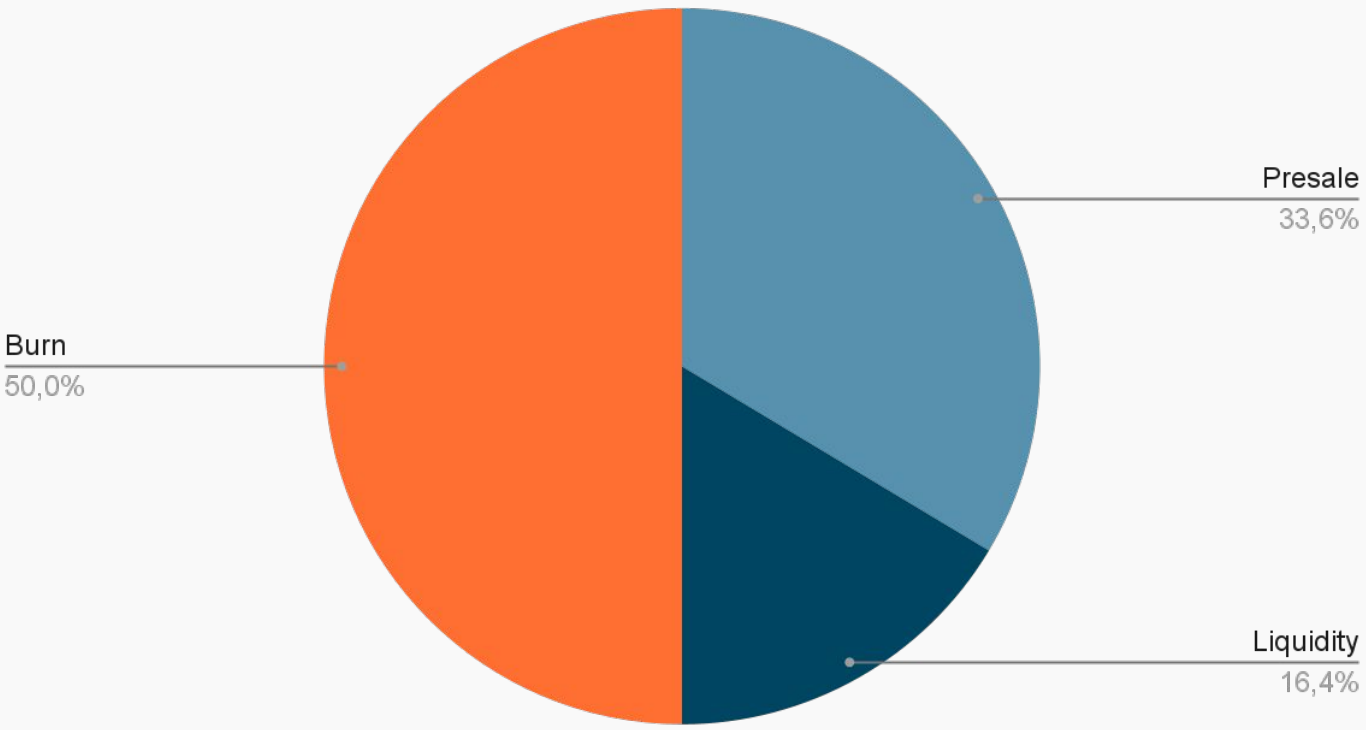
- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot set a transaction limit
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

- 33.6% - Presale
- 16.4% - Liquidity
- 50% - Burn

Tokens distribution



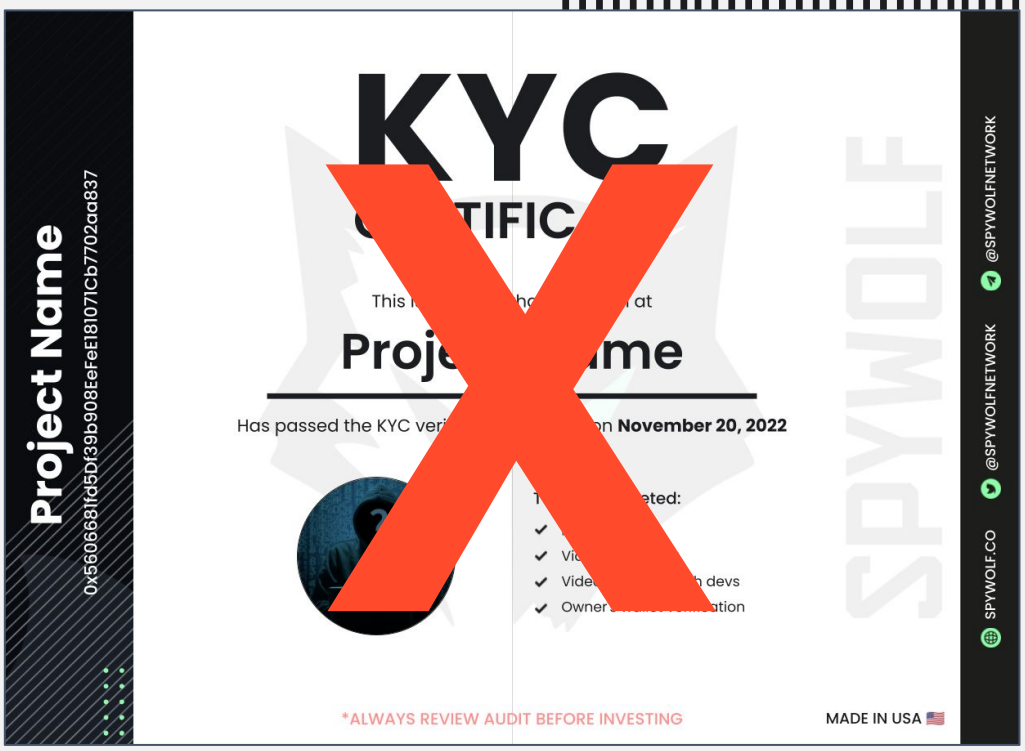
THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.



WEBSITE

Website URL
https://pandayaya.finance/

Domain Registry
https://www.namecheap.com/

Domain Expiration
2024-05-15

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Not very explanatory.

Roadmap
Yes, goals set without time frames.

Mobile-friendly?
Yes

pandayaya.finance

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

Project's social media pages are active

Twitter

@PandaYaYa_TK

- 1 126 followers
- 3 total posts

Discord

- Not available

Telegram

@PandaYaYaGroup

- 2 515 members
- Few active members
- Active mods

Medium

- Not available

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 500 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.